MONITORAPP

APPLICATION INSIGHT WAF-VE

Intelligent Web Application Firewall | AiWAF-VE

AIWAF-VE : Application Insight Web Application Firewall-Virtual Edition

웹 서버로 유입되는 트래픽을 검사하여 다양한 웹 공격으로부터 서버를 안전하게 보호하는 클라우드 전용 웹 어플리케이션 방화벽 입니다.

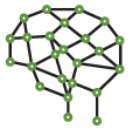
Why Do You Need a CLOUD WAF?

공개 웹 서버에 대한 위협

- 웹은 서비스를 위해 항상 개방 되므로 해커의 공격 위협에 노출
- 정보통신 기기 및 기술 등의 발달로 언제 어디서나 웹을 통한 주요 정보 접속 가능성 확대
- IDS, IPS 등 기존 네트워크 보안 솔루션의 한계에 따라 웹에 특화된 전문 솔루션 필요
- 웹 애플리케이션 해킹을 통한 DB 중요 정보 유출 가능성
- 보안 사고 발생시 회사 평판에 대한 부정적 영향 초래

클라우드 환경 최적화

- Kernel, Driver, TCP Stack 등 자체 개발 소프트웨어 사용으로 OS를 제외한 별도 요구 사항 없음
- 모든 Hypervisor 지원 : KVM, Xen, VMware ESX(i), MS Hyper-V 등
- 모든 Public / Private 클라우드 플랫폼 지원 : AWS, MS-Azure, GCP, Alibaba Cloud, NAVER Cloud, KT Cloud 등
- 웹 서버의 위치와 무관한 Reverser Proxy 모드로 동작
- Auto Scaling, HA(VRRP) 등 클라우드 환경 특성 지원



Machine Learning

Threat Intelligence

Web socket and API

WEB DLP

Bot

HTTP/2

Key Benefits of AIWAF-VE

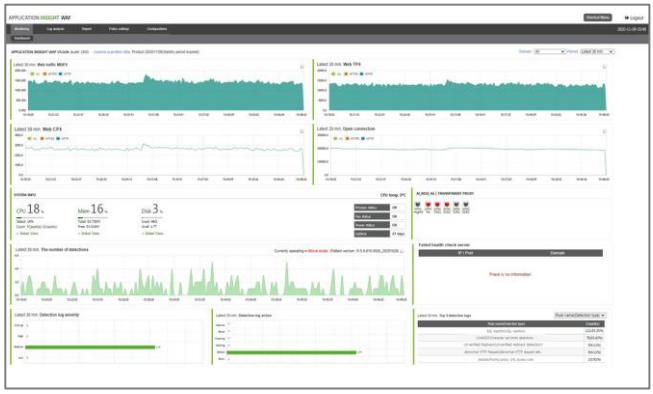
완전한 웹 서버 보안

- 요청 및 응답 데이터 구문 분석을 통한 포괄적인 웹 공격 탐지
  - SQL/LDAP Injection, XSS, CSRF, Web Shell, Overflow 등 요청기반 공격
  - Directory Listing, Error page 및 comment clocking 등 응답기반 공격
- Machine Learning & Threat Intelligence를 통한 Unknown 공격 대응
- 더블 & 멀티 인코딩 트래픽에 대한 디코딩 수행
- 주요 서버 정보 및 개인정보 유출 방지
- Script, Bot 등을 이용한 접속 트래픽 분석 및 탐지
- 웹 서버 응답페이지 분석을 통한 악성코드 검출 및 APT 대응
- 완전한 HTTP/2 연결 지원 및 HTTP/1.1과 동일한 보안 기능 제공

간편한 관리 및 운영

- HA (high availability) : active-standby
- 전체 또는 개별 웹 사이트 현황에 대한 통합 대시보드
- 도메인 별 차등적인 정책 설정 및 관리자 지정
- 탐지로그 내 요청/응답 데이터 로깅 및 탐지 근거 하이라이트 표기
- ESM, SNMP 등 모니터링 컨텐츠 커스터마이징
- HTTPS 인증서 관리 및 설정 자동화
- One-click 예외 처리, 오인탐지 정책 수립 자동 검증 등 다양한 운영 편의 기능
- 웹 서비스 품질향상을 위한 웹 캐시 및 QoS
- 서버 Health check 및 Load Balancing
- 복호화 된 HTTPS 트래픽을 3rd party 솔루션으로 전송

AIWAF-VE Administration GUI



1) 시스템 모니터링
> 실시간 시스템 상태 및 탐지, 트래픽 현황 모니터링
> 전체 또는 개별 웹 사이트 별 통합 대시보드 제공

2) 로그 분석
> 다양한 검색 조건을 통한 상세 로그 조회
> 탐지로그 내 요청/응답 본문 로깅 및 탐지 근거 하이라이트 표기

3) 정책 설정
> 도메인별 독립된 차등 정책 설정
> 각 개별 정책 및 패턴 별 IP, URL 기준 적용 또는 예외 대상 설정

Key Features of AIWAF-VE

1) 네트워크 구성모드
> Reverse Proxy

2) Passive Mirror
> 3rd Party 보안 솔루션으로 복호화 된 HTTPS 트래픽 전송

3) Threat intelligence 플랫폼
> AICC에 의한 실시간 위협 정보 업데이트
> proxy 경유, Black Client, C&C 트래픽 탐지

4) Machine Learning
> Machine Learning 기반 Unknown 공격 탐지
> 공격 트래픽 판별 및 각 정책 별 탐지확률 제시

5) Adaptive Profiling
> Self-Learning 엔진에 의해 정상 요청 및 응답 데이터에 대한 프로파일 데이터베이스 구축

6) Full HTTP/2 지원
> 완전한 HTTP/2 연결 및 구문 분석
> HTTP/1.1과 동일한 보안 기능 제공

7) ATP 대응
> 악성코드에 의한 경유지・유포지 악용 탐지
> 응답 데이터 본문 분석을 통한 악성코드 검출

8) 보안 최적화
> 오인 탐지 발생시 Rule별 예외 처리
> 정책 별 차단 페이지 차등 설정
> 각 개별 규칙 및 패턴에 대한 상세 제어
> 수립 정책에 대한 정탐/오탐 여부 셀프 테스트

9) 트래픽 최적화
> 웹 서비스 상태 및 품질 모니터링
> 서비스 상태에 따른 Server Load balancing
> 각 도메인별 QoS(Bandwidth Limit) 설정
> URL Rewrite (요청/응답)

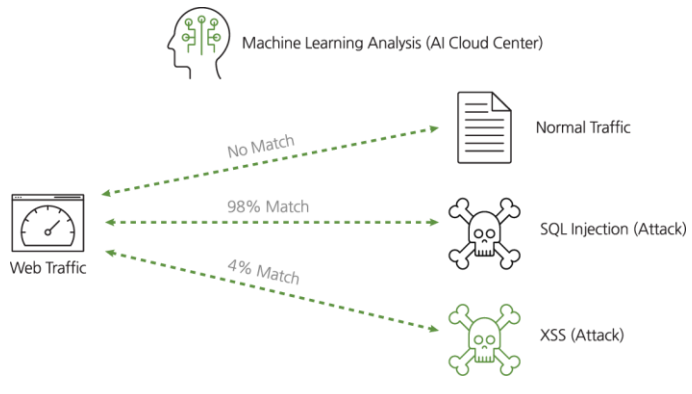
10) 웹 가속
> 웹 캐싱 기능을 통한 트래픽 절감 및 서비스 응답속도 향상

11) Bot 탐지
> Brute Force, Scraping, Denial of Inventory, Credential Stuffing 등에 사용되는 악성 Bot
> Java Script Injection, Human Interaction 등 다양한 메커니즘을 통한 Bot 트래픽 식별 및 탐지

12) Multi-Layer 웹 공격 대응
> Signature, Threshold Limit, Profiling 등
> 다양한 탐지 알고리즘을 통해 Injection, XSS 등
> OWASP TOP 10, HTTP Application DoS 등
> 이미 알려진 웹 공격에 대한 포괄적 방어

13) 패턴 업데이트
> 매월 정기 패턴 업데이트 제공
> 긴급 취약점 발생시 실시간 업데이트 및 공지

AICC for Machine Learning



Application Insight Cloud Center's Machine Leaning analysis of the request data is as follows: If it is determined to be an attack but is not detected by the current system, check that the policy or pattern is not used.

Analysis result : Maliciousness

Policy type	Attack
SQL injection	0.80129
Cross site script	0
CSRF detection	0
Command injection detection	0

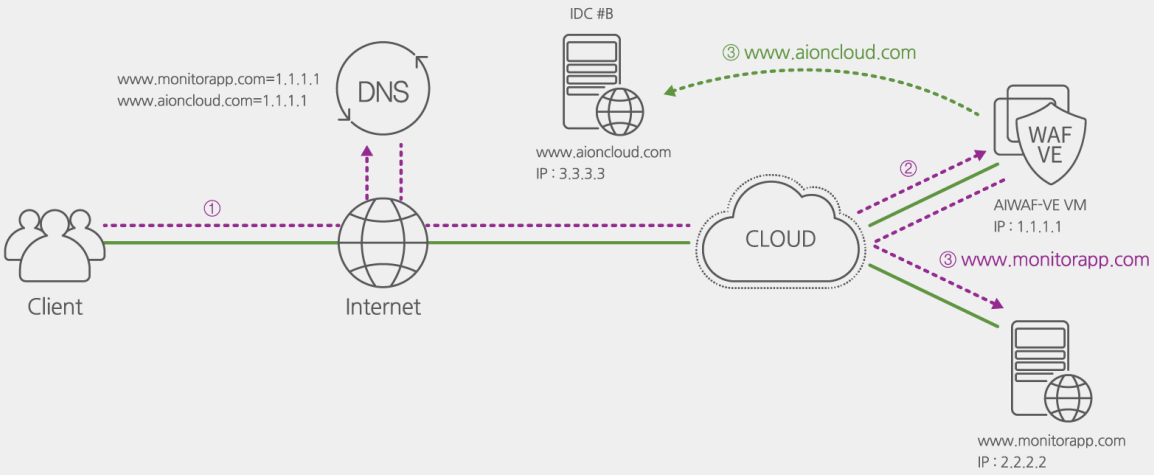
Detection policy | Export to Excel

The test results were detected by the following policies and rules. (2020-11-09 17:49:03)

Detected domain: Default Detection policy: 2Count(s) Detection rule: 2Count(s)

Classification	Policy	Rule name
Vulnerability attack detection	SQL injection	1
Abnormal request/response	Character set limits detection	CHARSET

AIWAF-VE Network deployment



Reverse Proxy

- 웹 서버의 위치와 무관한 Reverser Proxy 모드로 구성 되어, 분산 배치된 웹 서버군들에 대한 광범위 보호 수행
- 네트워크 경로나 DNS 주소 변경(A 레코드, CNAME)을 통해 AIWAF-VE로 트래픽 유입
- HA 구성 또는 DNS Failover를 통한 서비스 연속성 확보

AIWAF-VE Models & Specifications

- AIWAF Virtual Appliance 표준 워크로드를 기반으로 작성 되었으며, 실제 성능은 워크로드 요구 사항에 따라 크게 달라질 수 있습니다.

Specification	AIWAF-VE 01	AIWAF-VE 02	AIWAF-VE 04	AIWAF-VE 08	AIWAF-VE 16
CPU	2 Core	2 Core	4 Core	8 Core	16 Core
MEM	4 GB	8 GB	16 GB	32 GB	64 GB
HDD	500 GB	500 GB	500 GB	500 GB	1 TB
Max Support NIC	Multi	Multi	Multi	Multi	Multi
Max Throughput	100 Mbps	300 Mbps	500 Mbps	1 Gbps	2 Gbps
Notice	본 제품은 소프트웨어 타입으로 VM 및 이를 구성하는 물리 머신의 구성, 설정 등에 따른 성능 차이가 발생 합니다. 권장 규격으로서 CPU를 제외한 나머지 자원(MEM, HDD)은 필요에 따라 축소 될 수 있습니다. 최소 1개의 NIC가 필요하며, VM에 할당된 NIC는 모두 사용할 수 있습니다. (외부 네트워크/내부 네트워크 분리 목적 등)				

MONITORAPP
MONITORAPP CO., Ltd.
EMAIL sales@monitorapp.com
www.monitorapp.com